# Evaluating Password Advice

Hazel Murray
Department of Mathematics and Statistics
Maynooth University, Ireland
Email: hazelmsmurray@gmail.com

David Malone
Hamilton Institute
Maynooth University, Ireland
E-mail: david.malone@nuim.ie

***Abstract*—Password advice is constantly circulated by standards agencies, companies, websites and specialists. But there appears to be great diversity in terms of the advice that is given. Users have noticed that different websites are enforcing different restrictions. For example, requiring different combinations of uppercase and lowercase letters, numbers and special characters. We collected password advice and found that the advice distributed by one organization can directly contradict advice given by another. Our paper aims to illuminate interesting characteristics for a sample of the password advice distributed. We also create a framework for identifying the costs associated with implementing password advice. In doing so we identify a reason for why password advice is often both derided and ignored.**

## I. Introduction

Password advice is important for informing users and organizations about how to best maintain high standards of security. However, the content of the advice given is often not compatible across different sources. Our paper aims to understand the composition of the advice circulated to users and organizations and to identify key costs associated with the implementation of this advice. We collected a large selection of password advice and categorized it in order to highlight characteristics and discrepancies. Using the collected advice we were able to identify costs linked with implementing the advice. We believe this provides insight into why users and organizations are not enforcing researcher's recommended password practices.

In his 2009 paper, Herley [1] argues that users' rejection of security advice is rational from an economic perspective. Herley identifies advice relating to password security, phishing and certificate errors. For each, he discussed the costs and the potential/actual benefits. We will build on Herley's work through our creation of a framework for identifying the costs associated with enforcing password advice.

Despite the wide distribution of advice and the general acknowledgement of inconsistencies [2], a framework for simple analysis of advice is not available. Yet, many researchers have identified problems with the advice given [3]. Inglesant and Sasse [4] find that users are, in general, concerned with maintaining security but that existing security policies are too inflexible to match their capabilities, and the tasks and contexts in which they operate. We hope to develop this idea by identifying some of the demands associated with following passwords advice. Florêncio, Herley and van Oorschot [5] find that mandating exclusively strong passwords with no reuse gives users an effectively impossible task as portfolio size grows. Bellovin [6] questions whether simple adherence to password advice on security checklists really accomplishes the desired security goals. Florêncio, Herley and Coskun ask "Do strong web passwords accomplish anything?" [7]. They suggest that strength rules for web passwords accomplish very little when a lockout rule can restrict access. Beautement et al. [8] introduce the idea of a compliance budget which formalizes the understanding that users and organizations do not have unlimited capacity to follow new instructions and advice. This is an important concept for us to keep in mind when we look at the costs of implementing advice.

In this paper, Section II will explain how we collected the password advice and Section III illustrates the steps we took for categorizing it. Section IV describes our methods for identifying costs and how we assigned preliminary costs to a subset of the advice collected. Lastly, Section V discusses the characteristics associated with password advice which were highlighted during this process.

## II. Collection of Advice

To begin studying password advice, we first needed to collect a selection of the advice that is distributed to users. We primarily used Internet searches to collect password advice but also looked at advice given by standards agencies and multinational companies. We attempted to recreate the actions an individual or organization might take when seeking to inform themselves about proper password practices. As such, while the advice given in academic papers might be more considered, if it was not easily accessible, we did not include it in our study. In total, we collected 269 pieces of password advice from 21 different sources. Table I shows the types of sources from which the advice was gathered.

Table I
Break down of advice sources.

| Source | Number |
|---|---|
| Multinational companies | 6 |
| Universities | 6 |
| Security specialists | 5 |
| General articles | 4 |

This publication has emanated from research supported in part by a research grant from Science Foundation Ireland (SFI) and is co-funded under the European Regional Development Fund under Grant Number 13/RC/2077. This research is also supported by a John and Pat Hume doctoral studentship.

## III. Categorizing Advice

To extract meaning from the pieces of advice that we collected we subdivided the advice into categories. Within each category we created statements that generalized the recommendations pertaining to each category.

### A. Categorization

Our first step after collecting the advice was to group it into categories. For this we considered each piece of advice individually. The first pieces of advice we examined suggested our starting categories. From there, each piece of advice was either included in one of our existing categories, expanded the scope of an existing category or created a new category to suit it. For example, when approaching a piece of advice which said "Use a unique password for each of your important accounts" we created the category *Reuse across Accounts*. However, when a second piece of advice stated "Don't recycle passwords" we altered the name of the category to be the more general *Password reuse*. As an example, in Figure 1 we show the seventeen pieces of advice which became grouped under the category *Password reuse*.

In total, we identified 29 categories shown in Table II. The categories are listed in two columns; one showing categories containing advice aimed at users and the second showing advice aimed primarily towards organizations. Also included are the number of pieces of advice under each category. In this paper we only have space to include analysis of four of these categories. They are shown in italics in Table II.

We collected 155 pieces of advice aimed towards users and 114 pieces aimed towards organizations. Despite its greater quantity user advice has been subdivided into fewer categories. We speculate this could be related to the wider variety of roles an organization plays in the security of passwords. But it could also reflect our greater familiarity with user advice. While everyone is a user, not everyone has held all roles in an organization and therefore it was easier to interpret and categorize user advice.

### B. Classification into statements

Once we divided the advice into categories we noticed the pieces of advice within each category did not necessarily promulgate similar opinions. It was therefore necessary to subdivide the advice into statements which offer a similar message. In Figure 1 we can see how the seventeen pieces of advice under *Password Reuse* were grouped into three distinct statements:

- Never reuse a password.
- Alter and reuse passwords.
- Don't reuse certain passwords.

In this figure we make note of pieces of advice that contradict the main statement with a star (*). It is important to note that while it appears that there is no contradictory advice within the category statement "Never reuse a password" the third statement "Reuse certain passwords" is itself a contradiction. We make note of this by placing a star (*) in the text box of the third category. It is also represented by a star in Table IV. Already we are beginning to see inconsistencies with the advice that is circulated.

Table II
Categories and the quantity of advice they contain.

| **Users** | # | **Organisations** | # |
|---|---|---|---|
| *Phrases* | 37 | *Expiry* | 27 |
| *Composition* | 28 | Length | 17 |
| Personal Information | 21 | Storage | 13 |
| *Reuse* | 17 | Keeping system safe | 8 |
| Personal pwd storage | 17 | Throttling guesses | 8 |
| Backup pwd options | 8 | Individual accounts | 7 |
| Sharing | 14 | Generated pwds | 6 |
| Keeping account safe | 8 | Transmitting pwds | 2 |
| Password managers | 4 | Admin accounts | 4 |
| Username requirements | 2 | Default passwords | 4 |
| Two step verification | 1 | Shoulder surfing | 3 |
| Two factor authentication | 2 | Access to pwd file | 3 |
| | | Policies | 2 |
| | | Input | 3 |
| | | Network strings | 2 |
| | | Cracking | 1 |
| | | Back up work | 1 |
| **Total** | **159** | **Total** | **111** |

Thus, within each category we created generalized statements of the advice that was given. It is worth noting that the labels for advice are given from the perspective of the majority. For example, if two pieces of advice state that passwords should not include published phrases and one piece of advice states that it would be a good idea to use published phrases then the advice will be labeled as "Don't include published phrases".

The statements relating to the four chosen categories are shown on the left hand side of Table IV on page 5. For each statement the table shows how many pieces of the advice agree with the sentiment of the statement and how many disagree. This gives a clear indication of the inconsistencies in circulated password advice.

## IV. Identification of Costs

As described in Section III, we categorized the advice collected into 29 categories and 78 statements. For each statement, we identified the costs we believe are associated with it. Figure 2 shows an example for the statement "Passwords must not match account information".

We did not restrict ourselves in the types of costs we identified. In this way, we were not limiting ourselves by trying to stay within a predetermined structure. Despite this, we nearly immediately saw similarities in the costs we were identifying. After analyzing each of the 78 statements we had identified 10 categories of costs that we believe provide a rudimentary understanding of the general costs associated with obeying password advice. These are shown in Table III.

### A. Discussion of cost categories

When determining categories of costs we noticed that some categories are outcomes of others, similarly, many categories

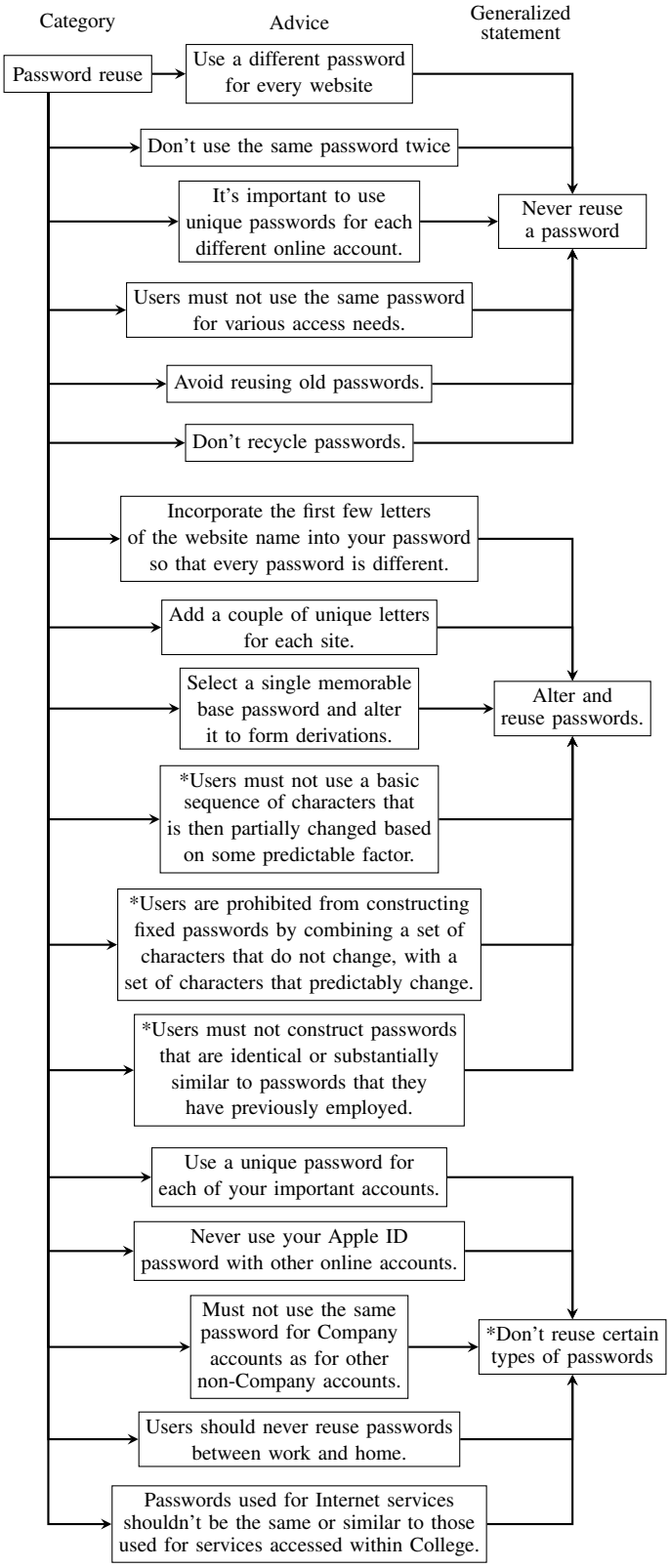


Figure 1. Method for categorizing advice. Example: Reuse.

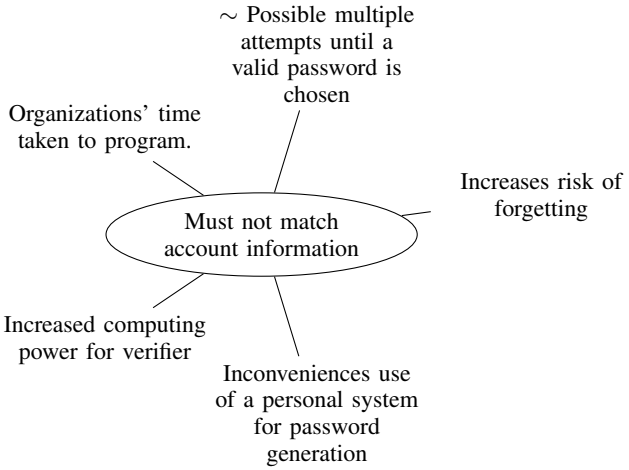


Figure 2. Identifying costs for the statement "Must not match account information".

Table III
COST CATEGORIES.

| | Costs |
|---|---|
| 1. | Increased risk of forgetting. |
| 2. | Need to pick a new password. |
| 3. | Possible multiple attempts needed to enter a valid password. |
| 4. | Inconveniences use of a personal system for password generation. |
| 5. | User time taken. |
| 6. | Reduced "entropy". |
| 7. | Organizations' time taken to enforce/program. |
| 8. | Impossible/hard to enforce. |
| 9. | Creates an additional security hole. |
| 10. | Increased computing power needed. |

can be seen to have "sub-costs". For example, *increased risk of resets* is a sub-cost of *increased risk of forgetting*. Similarly, *abandon site* can be seen as a result of *Possible multiple attempts needed to enter a valid password* and *irritating* [9] can be seen as an outcome of many of the other categories. In order to minimize this, we reduced the number of categories in the knowledge that we believe most categories will inevitably contain sub-costs. Note that we do keep *user time* as a distinct category as at times we recognize that there is no cost other than the users' time.

One of the cost categories we created was *Reduced "entropy"*. We are defining this to be a reduction in the number of guesses an attacker needs to make or a reduction in the keyspace or entropy (measure of uncertainty) [10][11]. We are not considering guesswork to be a substitute for entropy [12] but using the word "entropy" as a general word for guessability, keyspace and entropy. This is because relying solely on entropy oversimplifies how passwords withstand guessing attacks [3]. In many cases, the trade-off between keyspace/entropy/guessability is not clear and requires more information for a definitive answer.

We have presented the costs for the four selected categories

in Table IV. Each scheme is rated as either containing the cost (●) or not (no-circle); if a scheme contains some part of the cost or some variation of the cost, we use the "Quasi-" prefix (○) to indicate this. This is inspired by the system created by Bonneau et al. in their framework for analyzing password alternatives [13].

## V. Discussion

We will discuss some observations that we made for the chosen subset of advice categories. Depending on the category we will either discuss each statement in turn or consider the statements where the advice is unanimous and then the statements for which the advice is contradictory.

### A. Phrases

Advice regarding password phrases was the most commonly given advice we encountered. This implies that advice is mostly concerned with making passwords "strong". Yet in some cases, the strength of a password is irrelevant to defend users, as with password capture (e.g. phishing, keylogging) [3]. In fact, Bellovin 2008 [6] claims that the most common way passwords are compromised is via keylogger attacks.

*1) Unanimous:* Within the category *Phrases* there were no contradictions for the statements: *Don't use patterns, Take initials of a phrase* and *Don't use words.* The last is particularly interesting since from leaked password database we know users primarily chose word based passwords [14]. Shay et al. find that the "use of dictionary words and names are still the most common strategies for creating passwords" [15]. This depicts how ineffective some password advice can be and is possibly a reflection on the costs appearing to not outweigh the benefits from a users' point of view.

*2) Contradicting:* The statements: *Don't use published phrases* and *Substitute symbols for letters* had contradictions. For *don't use published phrases* the advice given was:

i "Don't use song lyrics, quotes or anything else that has been published."
ii "Do not choose names from popular culture."
iii "Choose a line of a song that other people would not associate with you."

The last piece of advice directly contradicts the first. This type of inconsistency in the advice given makes it no surprise that users seem disinclined to follow security advice [4][16].

The advice statement *Substitute symbols for letters* is proposed by two sources but is advised against by a third. We know from Warner [17] that passwords with simple character substitutions are weak. Yet, 2 of 3 pieces of advice recommend it. This could stem from the attitude that it is "better than nothing" and, as we can see from Table IV, the cost to the user is relatively low.

### B. Composition

Composition restrictions are regularly enforced by websites but the advice relating to this is not consistent from site to site. It is interesting to note that Herley [1] hypothesizes that different websites may deliberately have policies which are restrictive to different degrees. As this can help ensure that users do not share passwords between sites. Below we will discuss each of the three statements associated with composition.

*1) Must include special characters:* Seven sites instructed users to *include special characters* in their passwords, but five sites placed restrictions on the special characters that could be used. The main restriction on special characters was "do not use spaces". However, one piece of advice stated the more direct "do not use special characters". By not allowing users to include all special characters an attackers' search space is decreased.

*2) Don't repeat characters:* Not allowing the repetition of characters deters users from choosing passwords such as "aaaaaaa" or "wwddcc". Depending on the strictness of the restriction it could eliminate words such as "bookkeeper" or "goddessship". It could also cause some inconvenience for random password generators where the word "Sdt2htTtd65c8h" could be rejected. We list it as incurring the cost *reduced "entropy"* since it is banning characters sequences.

*3) Enforce restrictions on characters:* We collected twelve pieces of advice encouraging composition restrictions on passwords and only one piece of advice against it. The source rejecting composition rules was the NIST 2016 draft password guidelines. Though the guidelines are still in the review stage they are receiving promising responses from the research community [18]. This raises the question: will organizations begin to disseminate these new security practices? Or continue to enforce their stringent password restrictions?

We claim that forcing users to include special characters *quasi-reduces "entropy"*. If a user creates an eight digit passwords with no restrictions each of the eight characters could be any of the 96 possible ASCII characters. However, by restricting the password so that it must include one special character we limit the options for one of the character to the 34 special characters. This becomes more significant when a site enforces multiple restrictions on composition. In addition, the probability of a user including a "1" as their number and an "!" as there symbol is high [19]. So again an attacker can refine the guesses they make. This idea of composition restrictions reducing search space is something we will consider further in future work.

### C. Expiry

*1) Unanimous:* We found five pieces of advice telling organizations to *Store password history to eliminate reuse*, one encouraging organizations to *Enforce a minimum password age* and ten in favor of *Changing passwords if compromise is suspected.* If organizations do *store their users' password history* this *creates an additional security hole* as the company needs to allocate resources to protecting this file. Users can no longer reuse prior passwords but alterations are still possible [15]. In fact, Zhang, Monrose and Reiter [20] identify that we can easily predict new passwords from old when password aging policies force updates.

Table IV
COSTS OF IMPLEMENTING PASSWORD ADVICE.

| | # Against | # Supporting | Costs: Increased risk of forgetting | Need to pick a new password | Possible multiple attempts needed | Inconveniences use of personal system for password generation | User time | Reduced "entropy" | Organizations' time to enforce/program | Impossible/hard to enforce | Creates an additional security hole | Increased computing power needed |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phrases | | | | | | | | | | | | |
| Don't use patterns. | 0 | 6 | ● | | ● | ● | | | ● | ○ | | |
| Take initials of a phrase. | 0 | 4 | ○ | | | | | | | ● | | |
| Don't use published phrases. | 1 | 2 | ● | | | ○ | | | ● | ○ | | |
| Substitute symbols for letters. | 1 | 2 | ● | | | | | | | ● | | |
| Don't use words. | 0 | 16 | ● | | ● | ● | | | ● | | | |
| Composition | | | | | | | | | | | | |
| Must include special characters | 5 | 7 | ● | | ○ | | | ○ | ● | | | |
| Don't repeat characters. | 0 | 3 | ● | | ○ | ● | | ● | ● | | | |
| Enforce restrictions on characters. | 1 | 12 | ● | | ● | ● | | ○ | | | | |
| Expiry | | | | | | | | | | | | |
| Store history to eliminate reuse. | 0 | 5 | ○ | ● | ● | | | | ● | | ● | ● |
| Have a minimum Password Age. | 0 | 1 | | | | | | | ○ | | ○ | |
| Change your password regularly. | 4 | 7 | ● | ● | | | ● | ○ | ● | | | |
| Change if suspect compromise. | 0 | 10 | | ● | | | | | ○ | | | ○ |
| Reuse | | | | | | | | | | | | |
| Never reuse a password. | *5 | 6 | ● | ● | | | | | | ● | | |
| Alter and reuse passwords | 3 | 3 | ○ | | | | | | | ● | ○ | |
| Don't reuse certain sites' passwords. | 0 | 5 | | | | | | | | ● | ○ | |

●= requires the cost; ○= partially requires the cost; no circle = does not require the cost.

The reason given for introducing a *minimum password age* is to prevent users from bypassing the password expiry system by entering a new password and then changing it right back to the old one [21]. However, if an attacker gains access to a users' account and changes their password the user will be unable to change it again until the required number of days have elapsed, or with an administrators' help.

Ten pieces of advice recommended *changing passwords if a compromise is suspected*. This can be inconvenient for users not affected by the compromise, and also those that are. If there is a breach at the server the users were not at fault, yet still they must choose a new password.

*2) Contradicting:* From anecdotal evidence we know the advice *change your password regularly* is widely hated by users [22]. Referring to the costs in Table IV, we note that the costs associated with other advice are one-time occurrences. By contrast, when password expiry is enforced users face many of the costs periodically. Seven pieces of the advice we collected encouraged the use of password expiry while only four pieces of advice discouraged it. This is despite research suggesting that the security benefits are minimal [23][20]. This implies the inconvenience to users is worth less to organizations than the minimal security benefits. Or do organizations want to be seen to be enforcing strong security practices, and forcing expiry is just one way of doing this?

### D. Reuse

We collected six pieces of advice telling users to *never reuse passwords* and three pieces telling users to *not reuse passwords for certain sites*. In addition, we found three pieces of advice encouraging users to *alter and reuse their passwords* and three pieces telling users to not alter and reuse their passwords. There seems to be little agreement among the distributed advice in terms of password reuse.

*1) Never reuse a password vs. reuse for certain accounts:* Das et al. estimate that 43-51% of users re-use passwords across sites [24]. They also provide algorithms that improve an attacker's ability to exploit this fact. Florêncio, Herley and Van Oorschot [5] declare that, far from being unallowable, password reuse is a necessary and sensible tool for managing a portfolio of passwords. They recommend grouping passwords according to their importance and reusing passwords only within those groups. Interestingly, the advice we collected *Don't reuse certain passwords* gave a slightly different take on this advice. The advice mostly asked users to not use the password used for their site anywhere else e.g. "Never use your Apple ID password for other online accounts". Most organizations gave advice prioritizing their own accounts. Only one piece of advice suggested using a unique password for any important accounts [25].

*2) Alter and reuse passwords:* An alternative to grouping accounts for reuse is to alter and then reuse a password.

This advice was given by three sources and rejected by three sources. These alterations are sometimes very predictable. Using a cross-site password guessing algorithm Das et al. were able to guess approximately 10% of non-identical password pairs in less than 10 attempts and approximately 30% in less than 100 attempts. We could find no research identifying this method of altering and reusing passwords as effective. We consider altering and reusing passwords to *quasi-increase the risk of forgetting*, *impossible to enforce* and *quasi-creates an additional security hole*.

## VI. Conclusions

In this paper, we highlighted characteristics of the password advice currently available online. We show that there are serious discrepancies in the advice given between sources. We also note that some of the advice viewed by researchers and specialists as "best practice" is often not represented by the majority of advice. This contradictory information may reflect one of the reasons for users' unwillingness to follow advice.

We then looked at costs that could be associated with the enforcement of different pieces of password advice. Our aim here was to introduce the idea of a framework for deducing costs associated with implementing password advice. The costs model also provides some rudimentary insight into the biases of password advice.

Our collection and categorization of advice and identification of costs brought discrepancies in password advice into focus, in addition it highlighted the following interesting characteristics:

Research has shown that substituting symbols for letters is a weak security practice. But two of three pieces of advice recommend it.

Most of the advice we collected was concerned with making passwords strong. Yet, password strength cannot protect against password capturing malware, social engineering, or physical observation.

Of the 13 pieces of advice relating to password composition only the NIST 2016 draft guidelines spoke against restrictions.

Sixteen pieces of advice recommended that words not be included in passwords but we know from leaked password databases that users primarily choose word based passwords.

Seven pieces of the advice we collected encouraged the use of expiration policies while four discouraged it. The costs associated with expiry imply that the inconvenience to users is worth less to an organization that the minimal security benefits.

Similarly, most organizations gave advice encouraging the prioritization of passwords associated with their own accounts rather than encouraging realistic and user-focused security practices.

In terms of future work, our next step is to develop methods to quantify each of the costs we have identified in this paper.

## References


[1] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proceedings of the 2009 workshop on New security paradigms workshop*, pp. 133–144, ACM, 2009.

[2] J. Bonneau and S. Preibusch, "The password thicket: Technical and market failures in human authentication on the web.," in *WEIS*, 2010.

[3] L. Zhang-Kennedy, S. Chiasson, and P. van Oorschot, "Revisiting password rules: facilitating human management of passwords," in *Electronic Crime Research (eCrime), 2016 APWG Symposium on*, pp. 1–10, IEEE, 2016.

[4] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 383–392, ACM, 2010.

[5] D. Florêncio, C. Herley, and P. C. Van Oorschot, "Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts.," in *Usenix Security*, pp. 575–590, 2014.

[6] S. Bellovin, "Security by checklist," *IEEE Security & Privacy*, vol. 6, no. 2, pp. 88–88, 2008.

[7] D. Florêncio, C. Herley, and B. Coskun, "Do strong web passwords accomplish anything?," *HotSec*, vol. 7, no. 6, 2007.

[8] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 workshop on New security paradigms*, pp. 47–58, ACM, 2009.

[9] L. Klingbeil, "Password fatigue: Why users hate your site." https://blog.loginradius.com/2014/12/password-fatigue-why-users-hate-your-site/, 2014. Accessed: 2016-03-06.

[10] J. O. Pliam, "The disparity between work and entropy in cryptology," *ipi*, vol. 1, p. 1, 1998.

[11] J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," in *Security and Privacy (SP), 2012 IEEE Symposium on*, pp. 538–552, IEEE, 2012.

[12] D. Malone and W. Sullivan, "Guesswork is not a substitute for entropy," 2005.

[13] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Security and Privacy (SP), 2012 IEEE Symposium on*, pp. 553–567, IEEE, 2012.

[14] M. Weir, "The rockyou 32 million password list top 100.." reusablesec.blogspot.com/2009/12/rockyou-32-million-password-list-top.htmls, 2009. Accessed: 2017-02-14.

[15] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: user attitudes and behaviors," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, p. 2, ACM, 2010.

[16] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[17] C. Warner, "Passwords with simple character substitution are weak." https://optimwise.com/passwords-with-simple-character-substitution-are-weak/, 2010. Accessed: 2017-02-15.

[18] P. Cox, "Password sanity: Thank you NIST." https://www.linkedin.com/pulse/password-sanity-thank-you-nist-philip-cox, 2016. Accessed: 2016-12-15.

[19] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, "i added '!'at the end to make it secure": Observing password creation in the lab," in *Proc. SOUPS*, 2015.

[20] Y. Zhang, F. Monrose, and M. K. Reiter, "The security of modern password expiration: An algorithmic framework and empirical analysis," in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 176–186, ACM, 2010.

[21] Microsoft TechNet Magazine, "Best practices for enforcing password policies." https://technet.microsoft.com/en-us/library/ff741764.aspx. Accessed: 2016-12-06.

[22] J. Grobaski, "You hate changing your password and it doesn't help." https://epicriver.com/you-hate-changing-your-password-and-it-doesnt-help/, 2016. Accessed: 2016-03-06.

[23] S. Chiasson and P. C. Van Oorschot, "Quantifying the security advantage of password expiration policies," *Designs, Codes and Cryptography*, vol. 77, no. 2-3, pp. 401–408, 2015.

[24] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse.," in *NDSS*, vol. 14, pp. 23–26, 2014.

[25] Google, "Creating a strong password." https://support.google.com/accounts/answer/32040?hl=en. Accessed: 2016-12-17.